## AMENDMENTS

***In the Claims***

The following is a marked-up version of the claims with the language that is underlined ("___") being added and the language that contains strikethrough ("—") being deleted:

1. (Currently Amended) A method for blocking unsolicited e-mail transmitted to an e-mail server at an Internet Service Provider (ISP), the method comprising:

receiving a user identification (USERID) and a password associated with a customer;

retrieving a plurality of data associated with the customer based on the USERID and password;

authenticating the customer using the retrieved plurality of data;

dynamically adding an IP address assigned to the customer to a plurality of valid IP addresses associated with the ISP;

receiving SMTP traffic from the customer;

in response to receiving the SMTP traffic, determining, at the e-mail ~~server,~~ server, the e-mail server being configured to receive and maintain at least one e-mail, whether the customer is associated with a valid IP address; and

in response to determining that the customer is associated with a valid IP address, logging the customer onto the e-mail server using the IP address and the plurality of data used to authenticate the customer, wherein only the customer may access the mail server using the assigned IP address.

2. (Previously Presented) The method of claim 1, wherein authenticating the customer comprises:

receiving the USERID and password associated with the customer to an authentication ISP;

comparing the USERID and password against at least one USERID and password associated with at least one registered user of the ISP;

generating a negative response if the USERID and password associated with the customer does not match a USERID and password associated with at least one registered customer;

generating a positive response if the USERID and password associated with the customer matches a USERID and password associated with at least one registered customer; and

receiving a START record, the START record indicating the beginning of the customer's access to the e-mail server.

3. (Previously Presented) The method of claim 1, wherein the plurality of IP addresses are used only by customers registered with the ISP to access the Internet through a remote server.

4. (Previously Presented) The method of claim 1, wherein dynamically adding the customer's IP address to a pool of valid IP address comprises:

reading a START record, a timestamp, a RELAY from the database; and

forwarding a START record, USERID, password, and IP address for adding the IP address to the pool of valid IP addresses.

5. (Previously Presented) The method of claim 1, wherein logging the customer onto the e-mail server comprises:

initiating an SMTP request to send e-mail from an e-mail application server; and

validating the IP address of the customer against the pool of valid IP addresses.

6. (Previously Presented) The method of claim 1, further comprising logging off the customer from a remote server.

7. (Previously Presented) The method of claim 6, wherein logging off the customer, comprises:

receiving a termination signal by the customer;

transmitting the customer's USERID to the remote server to identify the customer to be logged off; and

receiving a STOP record, wherein the STOP record is operable to identify the customer.

8. (Previously Presented) The method of claim 7, wherein receiving the STOP record further comprises determining whether the customer has sent any unauthorized email messages.

9. (Currently Amended) A method of preventing unsolicited e-mails from being transmitted via a mail server associated with the Internet Service Provider (ISP) of a ~~customer:~~ customer, the method comprising:

receiving a user identification (USERID) and password, wherein the USERID and password are associated with the customer;

authenticating the customer as a registered user of the ISP;

generating a positive response if the customer is a registered user of the ISP;

receiving a START record indicating that the customer is being logged onto a Network Access Server (NAS);

writing the START record to a database;

receiving SMTP traffic from the customer for delivery to a recipient;

in response to receiving the SMTP traffic determining, at the mail ~~server,~~ server, the mail server being configured to receive and maintain at least one e-mail message, whether an IP address assigned to the customer is valid; and

in response to determining that the IP address assigned to the customer is valid, forwarding the SMTP traffic to the recipient.

10. (Previously Presented) The method of claim 9, further comprising generating a negative response if the customer is not a registered user at the ISP.

11. (Previously Presented) The method of claim 10, wherein generating a negative response comprises denying the customer access to the Internet through the NAS.

12. (Previously Presented) The method of claim 9, wherein the START record comprises an IP address, a protocol, a port type, a User name, a called station ID, a calling station ID, an account status type, an account authentication, a service type, an account session ID, a framed protocol, an account delay time, and a start timestamp.

13. (Previously Presented) The method of claim 9, wherein the database contains data organized according to a Terminal Access Controller Access Control System (TACACS) format.

14. (Previously Presented) The method of claim 13, wherein the database has been modified to include a USERID field.

15. (Currently Amended) A method of logging on a customer of an Internet Service provider (ISP) onto a mail server while preventing the unauthorized distribution of SPAM messages via the mail server, the method comprising:

authenticating that the customer is a registered customer of the ISP;

storing a data log in a database, the data log comprising a plurality of attributes to track the customer's usage of the network connection;

receiving SMTP traffic from the customer;

in response to receiving the SMTP traffic, determining, at the mail ~~server,~~ server, the mail server being configured to receive and maintain at least one e-mail message, whether as IP address assigned to the customer is valid; and

in response to determining that the IP address assigned to the customer is valid, connecting the customer to the mail server using the IP address.

16. (Previously Presented) The method of claim 15, further comprising removing the IP address from a list of at least one valid IP address upon receiving a command to log off the customer from mail server.

17. (Previously Presented) The method of claim 15, wherein authenticating the customer comprises:

receiving a user identification (USERID) and a password associated with the customer;

comparing the USERID and password from the customer to a list of at least one USERID and password associated with at least one registered customer of the ISP;

transmitting a positive response if the USERID and password associated with the customer matches a USERID and password associated with a registered customer from the list; and

transmitting a negative response if the USERID and password does not match a USERID and password associated with at least one registered customer of the ISP from the list of at least one USERID and password stored at the authentication server.

18. (Previously Presented) The method of claim 15, further comprising, creating a data log associated with the customer, wherein the data log comprises a START identifier, the USERID and password associated with the customer, the IP address assigned to the customer, a RELAY to the mail server from a Network Access Server (NAS), and a timestamp indicating the starting time the customer logged onto the mail server.

19. (Previously Presented) The method of claim 1, further comprising assigning an IP address to the customer.

20. (Previously Presented) The method of claim 7, further comprising transferring the USERID to an authentication server on the ISP.

21. (Previously Presented) The method of claim 9, further comprising transmitting the USERID and password from the Internet device to the NAS.

22. (Previously Presented) The method of claim 9, further comprising assigning a local IP address to the customer, the local IP address being selected from a plurality of IP addresses at the NAS.

23. (Previously Presented) The method of claim 11, further comprising not allowing the customer to authenticate.

24. (Previously Presented) The method of claim 12, wherein the START record comprises a NAS IP address, a NAS protocol, a NAS port type, a User name, a called station ID, a calling station ID, an account status type, an account authentication, a service type, an account authentication, a service type, an account session ID, a framed protocol, an account delay time, and a start timestamp.

25. (Previously Presented) The method of claim 15, further comprising transferring the data log to a mail access server at the ISP.

26. (Previously Presented) The method of claim 15, further comprising assigning an IP address to the customer to access the mail server.

27. (Previously Presented) The method of claim 26, further comprising adding the IP address assigned to the customer to a list of a valid IP address that are allowed to access the mail server on the ISP.